ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

АНАЛІЗ ТА ОЦІНКА ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ /
ANALYSIS AND EVALUATION OF VULNERABILITIES OF INFORMATION SYSTEMS

СИЛАБУС/
SILABUS

ЗАТВЕРДЖЕНО
засіданням кафедри
(протокол №. 1
від «04» серпня 2024 р.)
завідувач кафедри
_____Олена КРИВОРУЧКО

Київ 2024

Назва освітньої компоненти	**АНАЛІЗ ТА ОЦІНКА ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ /** ANALYSIS AND EVALUATION OF VULNERABILITIES OF INFORMATION SYSTEMS
Спеціальність	125 «Кібербезпека»
Освітній ступінь	Перший (бакалавр)
Освітньо-професійна програма	**БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ В ЕКОНОМІЦІ**
	Лектор: **Криворучко Олена** -завідувач кафедри інженерії програмного забезпечення та кібербезпеки, гарант освітньої програми «Комп'ютерні науки» (PhD) -доктор технічних наук -пофесор Резюме викладача: https://knute.edu.ua/blog/read/?pid=39648&uk Науковий профіль: https://knute.edu.ua/blog/read/?pid=46714 е-пошта: kryvoruchko_ev@knute.edu.ua
	Асистент лектора: **Сергій Бульба** -ст.викладач, гарант освітньої програми «Інженерія програмного забезпечення» -к.е.н. Резюме викладача: https://knute.edu.ua/blog/read/?pid=48084&uk Практична діяльність: Senior System Analyst, Solution Architect е-пошта: s.bulba@knute.edu.ua
Консультації	https://knute.edu.ua/blog/read/?pid=47103&uk
Програма освітньої компоненти	https://knute.edu.ua/blog/read/?pid=48215
ЗМІСТ ОСВІТНЬОЇ КОМПОНЕНТИ	
Тема 1. Технічний аудит інформаційних систем	Поняття технічного аудиту інформаційних систем. Суть, види, зміст. Основні етапи аудиту впровадження інформаційних систем. Перевірка відповідності інформаційної системи очікуванням. Наскрізне тестування інформаційних систем. Перевірка надійності і безпеки програмного забезпечення. Сфери здійснення аудиту інформаційних систем. Основні види тестування надійності ПЗ. Етапи підготовки та моніторингу

	для тестування надійності. Методології та підходи до оцінювання захищеності інформаційних систем. Кількісні та якісні методи аналізу захищеності. Відповідальність за порушення законодавства у сфері кібернетичної безпеки
Тема 2. Збір інформації з відкритих джерел	Розвідка. Етичний хакінг. Тестування захищеності (Penetration Testing). Типи тестування захищеності. Етапи тестування захищеності. Сервери C&C (керування та контролю) та їх використання для моніторингу мереж. Складові кібернетичної розвідки. Етапи проведення кібернетичної розвідки. Рекогносцировка. Сканування мережі. Відкрите сканування. Напіввідкрите сканування. Приховане сканування. Ping-комбінації. Отримання доступу. Підтримка доступу. Приховування слідів присутності. Аналітичний звіт. Методології та програмні засоби. Пасивний метод збору розвідувальних даних. Активний метод добування розвідувальних даних.
Тема 3. Аналіз та оцінка вразливостей мережевих ресурсів	Типи мережевих атак. Сніффер пакетів. Методи протидії сніф-фінга пакетів: аутентифікація, комутована інфраструктура, антисніффери, криптографія. IP-спуфінг. Методи протидії спуфінгу: контроль доступу, фільтрація RFC 2827, аутентифікація. Парольні атаки. Атаки на рівні застосунків. Мережева розвідка у формі запитів DNS, exo-тестування (ping sweep) і сканування портів. Соціальна інженерія. Пошук цілей та вразливостей мережевих ресурсів (NETWORK). Перехоплення трафіку та Man in the middle (MITM). Експлуатація знайдених вразливостей. Можливі дії після успішної експлуатації. Аналіз вразливостей хмарних технологій.
Тема 4. Аналіз та оцінка вразливостей комп’ютерних систем	Суть та основні поняття System security. Криптографія та па-рольні атаки. Переповнення буферу та інші види вразливостей систем. Класифікація атак. За характером впливу (пасивні та активні). За метою впливу (порушення конфіденційності, цілісності, доступності). За умовою початку здійснення впливу (з настанням події, що очікується на об’єкті, та безумовна атака). За наявністю зв’язку з об’єктом, що атакується (зі зворотнім зв’язком та односпрямована атака). За розташуванням об’єктів атаки (всередині сегментна та міжсегментна). За кількістю атакуючих (розподілена та нерозподілена). Критерії захищеності інформації в комп’ютерних системах від несанкціонованого доступу. Побудова і структура критеріїв захищеності інформації. Критерії конфіденційності. Критерії цілісності. Критерії доступності. Критерії спостереженості. Критерії гарантій. Системи виявлення атак.
Тема 5. Аналіз та	Суть та основні поняття WEB-pentesting. Збір інформації та

оцінка вразливостей WEB-ресурсів	розвідка. Забезпечення безпеки WEB-застосунків. Вивчення об'єкта. Пе-ревірка параметрів безпеки WEB-серевера. Дослідження застосунків. Оцінка вразливостей WEB-ресурсів. Проникнення. Аутентифікація. Авторизація. Аналіз та оцінка вразливостей засобів управління сеансом. Аналіз засобів перевірки введених даних. Аналіз сховищ даних та WEB-служб. Аналіз засобів управління WEB-затосунками та використанні WEB-клієнтів. Ін'єкції, інші види вразливостей та способи атак на WEB-ресурси. Політика реалізації послуг безпеки інформації WEB-сторінки.
Тема 6. Аналіз та оцінка вразливостей бездротових мереж Wi-Fi	Необхідне обладнання та налаштування середовища. Стандарти бездротових мереж. Ad-hoc (бездротові самоорганізовані мережі). Hot-spot (бездротові керовані мережі). Дослідження Wi-Fi мереж, аналіз трафіку, атаки на бездротові мережі. Механізми захисту Wi-Fi мереж. Методи автентифікації клієнтів. Відкрита автентифікація та автентифікація із загальним ключем. WPA та WPA2. Методи шифрування даних. WEP-шифрування. WPA-шифрування. WPA2-шифрування. Протокол WPS. Застосування віртуальної приватної мережі VPN. Використання протоколу SSL.
Тема 7. Аудит управління неперервністю бізнеса в економіці	Аудит інформаційної безпеки. Процесний підхід до інформаційної безпеки. Правові та методологічні основи аудиту інформаційної безпеки. Усвідомлення та менеджмент аудиту інформаційної безпеки. Методи оцінювання інформаційної безпеки. Дослідження отриманих оцінок інформаційної безпеки. Методології, стандарти та нормативні вимоги в області управління неперервністю бізнеса. Документування дій аудитора щодо аналізу та оцінювання вразливостей інформаційних систем. Написання звіту на основі проведеного аналізу інформаційних систем.

СПИСОК ОСНОВНИХ РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.
2. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем. Підручник. – К.: вид. ДУІКТ, 2010. - 316 с.
3. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Підручник. / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К.: ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
4. Андрєєв В.І., Хорошко В.О., Чередніченко В.С., Шелест М.Є. Основи інформаційної безпеки. Підручник. – К.: вид. ДУІКТ, 2009. –292 с.

Додатковий

5. Цимбалюк В.С. Інформаційне право (теорія і практика). Монографія. – К.: 2009. 364 с.
6. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки. /

Невойт Я.В., Єрмошин В.В.// Монографія. – К: ДУТ, 2015. – 124 с.
7. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.
8. Бабак В.П. Теоретичні основи захисту інформації : підручник // Бабак В.П. – Книжкове видавництво НАУ, 2008. – 752 с.
9. Основи захисту інформації : навч. посібн. / О.А. Смірнов, Л.Г. Віхрова, С.І. Осадчий та ін. – Кіровоград, 2010. – 322 с.
10. Основи інформаційної безпеки / С.В. Кавун, О.А. Смірнов, В.Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.
11. Блінцов В.С. Захист програмних продуктів : навчальний посібник / В.С. Блінцов, С.С. Козирев. – Миколаїв : НУК, 2010. – 146 с.
12. Голубєв В. О. Інформаційна безпека : проблеми боротьби з кіберзлочинами : монографія / В.О. Голубєв. – Запоріжжя : ГУ «ЗІДМУ», 2003. – 250 с.
13. Інформаційний та кіберпростори : проблеми безпеки, методи та засоби боротьби : посібник / В.Л. Бурячок, С.В. Толюпа, В.В. Семко та ін. – К. : ДУТ – КНУ, 2016. – 178 с.
14. Кавун С. В. Інформаційна безпека : підручник / С. В. Кавун. – Харків: Вид. ХНЕУ, 2009. – 368 с.
15. Конахович Г.Ф. Захист інформації в мережах передачі даних : підручник / Г.Ф. Конахович. – К. : Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714 с.
16. Кузнецов О.О. Захист інформації в інформаційних системах / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2011. – 512 с.
17. Остапов С.Е. Технології захисту інформації : навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
18. НД_2.5_004_99. Критерії оцінки захищеності інформації в комп'ютерних системах.
19. НД_2.5_005_99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності.
20. Державна служба спеціального зв'язку та захисту інформації України http://www.dsszzi.gov.ua/dsszzi/control/uk/index
21. Офіційний вебпортал парламенту України http://www.rada.gov.ua

РЕЗУЛЬТАТИ ВИВЧЕННЯ ОСВІТНЬОЇ КОМПОНЕНТИ

Дисципліна забезпечує оволодіння здобувачами вищої освіти загальними та фаховими компетентностями і досягнення ними програмних результатів навчання:

КЗ1	Здатність застосовувати знання у практичних ситуаціях.
КЗ2	Знання та розуміння предметної області та розуміння професії.
КЗ4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
КФ8	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
КФ9	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
КФ12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та

	інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
КФ14	Здатність здійснювати управління ризиками інформаційної та кібербезпеки.

ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ ОСВІТИ

Сума балів, накопичених здобувачем вищої освіти за виконання всіх видів поточних навчальних завдань (робіт) на лабораторних/практичних заняттях, свідчить про ступінь оволодіння ним програмою освітньої компоненти на конкретному етапі її вивчення. Протягом семестру здобувачі освіти можуть набрати від 0 до 100 балів, що переводяться у національну шкалу оцінювання і відповідно у шкалу ЄКТС. Кількість балів відповідає певному рівню засвоєння дисципліни

Довідник з розподілу оцінок ДТЕУ (Шкала ЄКТС):

Бали ДТЕУ	Відсоток балів відносно загальної кількості одержаних прохідних балів	Кумулятивний відсоток отриманих прохідних балів
90-100	20	20
82-89	10	30
75-81	20	50
69-74	10	60
60-68	40	100

Роподіл балів за видами робіт:

Вид роботи	**Бали**	**Вид роботи**	**Бали**
Лабораторна робота 1	10	Самостійна робота 1	5
Лабораторна робота 2	10	Самостійна робота 2	5
Лабораторна робота 3	10	Самостійна робота 3	5
Лабораторна робота 4	10	Самостійна робота 4	5
Лабораторна робота 5	10		
Додаткові бали	20	Наукова робота	10

Вимоги до критеріїв оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)

40%	Детальний розгляд сутності та вмісту основних джерел. Подання фактів, ідей і результатів досліджень у логічній послідовності. Правильно проаналізовано поточний стан дослідження проблеми та зроблено огляд перспектив подальшого розвитку даного питання.
40%	Обґрунтованість аргументів, підтвердження особистого ставлення, пропозиції стосовно вирішення завдання, встановлення напрямків аналізу.
20%	Оформлення звіту у відповідності вимог

Критерії оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)

100%	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних

	виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
80%	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань
60%	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
40%	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та лабораторних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
20%	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.
0%	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.
ОСНОВНІ ПОЛОЖЕННЯ, ЩО РЕГЛАМЕНТУЮТЬ ОСВІТНІЙ ПРОЦЕС	
діючі положення	https://knute.edu.ua/blog/read/?pid=44402
нормативно-правова база організації освітнього процесу	https://knute.edu.ua/blog/read/?pid=7330&uk
студенту	https://knute.edu.ua/#forstudent
НЕФОРМАЛЬНА ОСВІТА Рекомендовані сертифікаційні програми, курси, посібники користувача	
Qualys Community: Certified Course: Vulnerability Management Foundation	https://www.qualys.com/training/course/vulnerability-management-foundation/

Vulnerability Assessment	https://www.udemy.com/course/vulnerability-assessment-and-penetration-testing/?couponCode=ST17MT91224B
Vulnerability Management - From Beginner To Mastery	https://www.udemy.com/course/vulnerability-management-from-beginner-to-mastery/?couponCode=ST17MT91224B
Cisco Academy: Introduction to cybersecurity	https://shorturl.at/jg4Nj
Udacity: System Security	https://shorturl.at/COs1n
ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ:	
Відвідування лекційних та лабораторних занять: відвідування	Відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).
Відпрацювання пропущених занять:	відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).
Правила поведінки під час занять	обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття. Задля зручності, дозволяється використання ноутбуків та інших електронних пристроїв під час навчання в комп'ютерних аудиторіях (за взаємною згодою всіх учасників освітнього процесу)
Політика академічної доброчесності ДТЕУ	https://knute.edu.ua/blog/read/?pid=38987&uk